IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

NO. 5:20-CR-00464-D

UNITED STATES OF AMERICA	)	
	)	UNITED STATES' RESPONSE
v.	)	IN OPPOSITION TO
	)	DEFENDANT'S MOTION TO
WILLIAM ROBERT JEFFERY	)	SUPPRESS

The United States of America, by and through the United States Attorney for the Eastern District of North Carolina, hereby responds in opposition to the defendant's motion to suppress evidence, filed November 16, 2021 (DE 45, "Mot.").

The residential search warrant in this child exploitation case relied on two images that Microsoft reported to the National Center for Missing and Exploited Children ("NCMEC"). Because the defendant uploaded the images for review by a search engine and subject to Microsoft's privacy policy, he had no reasonable expectation of privacy. Even if he had, Microsoft lawfully scanned and reviewed the defendant's uploads as a private actor, and neither NCMEC nor law enforcement expanded the scope of Microsoft's initial private search. The motion should be denied.

FACTS AND PROCEDURAL HISTORY

On October 19, 2019, and again on January 3, 2020, NCMEC received CyberTipline Reports from Microsoft BingImage, an electronic service provider ("ESP"), indicating that a user with an Internet Protocol ("IP") address from Raleigh,

North Carolina, had uploaded images of child pornography. Ex. 1 (CyberTipline Report 57356024); Ex. 2 (CyberTipline Report 62299605).

Bing Visual Search, or BingImage, is a Microsoft service through which a user can upload an image to find similar images. Ex. 3 ¶ 8 (Microsoft Declaration, December 8, 2021). Microsoft scans the uploads using PhotoDNA—"an industry-leading image-matching technology developed by Microsoft in collaboration with Dartmouth College that helps Microsoft, along with more than 300 other companies and organizations across the globe, find and remove images of child sexual exploitation and abuse from online services." *Id.* ¶¶ 5, 9. "PhotoDNA uses a mathematical algorithm to create a unique signature—similar to a fingerprint—for each digital image." *Id.* ¶ 6. The signature for known images of child abuse "can be compared with the signatures of other images to find copies of the original illicit image." *Id.* This process is called "hashing." *Id.* ¶ 7; *see also United States v. Reddick*, 900 F.3d 636, 639 (5th Cir. 2018) ("Hash value comparison allows law enforcement to identify child pornography with almost absolute certainty, since hash values are 'specific to the makeup of a particular image's data." (internal quotation marks omitted)).

Microsoft performs these scans "to ensure the safety of Bing.com, including the Bing Visual Search function," *id.* ¶ 8, and to avoid "direct and indirect costs resulting from the presence" of child exploitation images on its services, *id.* ¶ 2. Scanning is especially important for Bing Visual Search because the service retains uploaded images "to train Microsoft's image-matching algorithm." *Id.* ¶ 8. Without the

PhotoDNA scans, Microsoft would keep illicit images on its servers and could then "match and surface images of child sexual abuse." *Id.*

When Microsoft confirms that a user has uploaded a child sexual abuse image to Bing Visual Search, it files a CyberTipline Report with NCMEC, containing information about the file and associated IP addresses. *Id.* ¶ 9. Through the report, Microsoft is able to "prevent the image from being transmitted, protect its customers, and comply with U.S. law." *Id.* While federal law does not require a service provider to investigate violations of child pornography laws, it does require reporting to NCMEC when a provider "obtains actual knowledge of any facts or circumstances" indicating violations of certain enumerated offenses. 18 U.S.C. § 2258A.

Relevant to this case, Microsoft BingImage submitted at least five CyberTipline Reports to NCMEC regarding uploads from the same Raleigh IP address. Two reports were the subject of the initial investigation and search warrant. On October 19, 2019, NCMEC received CyberTipline Report 57356024, in which Microsoft notified NCMEC that a user with the Raleigh IP had uploaded one image depicting the lascivious exhibition of a nude pubescent minor. Ex. 1, at 4, 6. Then on January 3, 2020, NCMEC received CyberTipline Report 62299605, in which Microsoft stated that the same Raleigh IP had uploaded one image depicting a pubescent minor engaged in a sex act. Ex. 2, at 4, 6. In both instances, Microsoft confirmed that it had "view[ed the] entire contents of [the] uploaded file." Ex. 1, at 4; Ex. 2, at 4; Ex. 3 ¶ 10. With each report, Microsoft uploaded only the single image to NCMEC. Ex. 4 ¶ 13 (NCMEC Declaration for CyberTipline Report 57356024); Ex.

5 ¶ 13 (NCMEC Declaration for CyberTipline Report 62299605). Both times, NCMEC staff viewed and confirmed the image to be "Apparent Child Pornography." Ex. 1, at 8; Ex. 2, at 8; Ex. 4 ¶ 17; Ex. 5 ¶ 17.

NCMEC then forwarded the reports to the North Carolina State Bureau of Investigation and the Internet Crimes against Children ("ICAC") Task Force, who referred the information to FBI Task Force Officer Zeke Morse. TFO Morse reviewed the CyberTipline Reports in March 2020 and, like Microsoft and NCMEC before him, confirmed that the attached images depicted child sexual abuse material. AT&T IP address records linked the IP address to subscriber William Jeffery and a residence in Raleigh.

On March 17, 2020, TFO Morse obtained a state search warrant for the defendant's residence, relying on the CyberTipline Reports and his review of the two images. Ex. 6, at 6-7 (Residential Search Warrant). Law enforcement executed the warrant on the same day, seizing a 1-terabyte hard drive from a laptop and a 30-gigabyte hard drive from a desktop computer. During an interview, Jeffery stated, "I am not going to tell you that young girls are not attractive, because they are. Beautiful." He denied possessing child pornography but admitted that he deleted his internet history daily. A subsequent forensic examination of Jeffery's devices revealed 57 images of child sexual abuse material, along with 336 images categorized as child exploitative or age difficult.

On November 2, 2020, a federal grand jury returned a single-count superseding indictment charging the defendant with possession of child pornography, in violation

of 18 U.S.C. § 2252A(a)(5)(B). On November 16, 2021, the defendant filed the pending motion to suppress. The arraignment is scheduled for the February 7, 2022 term of court.

ARGUMENT

I. The defendant had no reasonable expectation of privacy in images that he uploaded specifically for Microsoft to review

The Constitution does not prohibit all searches and seizures, but only those that are unreasonable. *Elkins v. United States*, 364 U.S. 206, 222 (1960); U.S. Const. amend IV (protecting "against unreasonable searches and seizures"). Outside the context of physical trespass, a "search" within the meaning of the Fourth Amendment occurs when governmental action infringes on "an expectation of privacy that society is prepared to consider reasonable." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

If there is no recognizable expectation of privacy in the area searched, the Fourth Amendment protections are not implicated. "The burden of showing a reasonable expectation of privacy in the area searched rests with the defendant." *United States v. Gray*, 491 F.3d 138, 144 (4th Cir. 2007). To carry that burden, a defendant must establish that he had "a legitimate expectation of privacy in the place searched or the item seized," and that "his subjective expectation of privacy is one that society is prepared to accept as objectively reasonable." *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000).

The defendant's use of Bing's Visual Search feature in this case is incompatible with any reasonable expectation of privacy. He uploaded the two files at issue

intending for Microsoft to review them and to find similar images; that's the Visual Search service's basic purpose. Ex. 3 ¶ 8. This process involved scanning through PhotoDNA, comparison through Microsoft's image-matching algorithms, and in the cases of non-contraband files, retention on the servers to train the algorithm. *Id.* He may not have known the specifics, but one way or another, the defendant knew that Microsoft would have to review the files to find the similar images he sought. This is not a case where someone simply stored a private file in a personal account. In addition, and more generally, the Microsoft Service Agreement and Privacy Statement explain that "some of our products … systematically scan content in an automated manner to identify … abusive actions." *Id.* ¶ 4. Far from expecting privacy, the defendant knew that Microsoft would scan his uploaded image. There can be no Fourth Amendment violation.

II. Microsoft is a private actor, and its conduct does not implicate the Fourth Amendment

Regardless of privacy expectation, the Court should also deny the defendant's motion because Microsoft's private search of the defendant's uploads does not implicate his Fourth Amendment protections. His theory that Microsoft is a government agent is unfounded in fact or law.

The Fourth Amendment is "wholly inapplicable" to a search or seizure conducted by a private party, so long as the party is not acting as an agent of the government. *Jacobsen*, 466 U.S. at 113. And after a private search, "additional invasions of . . . privacy by the government" are lawful if they stay within the scope of the private search. *Id.* at 115.

The Fourth Amendment does, however, "protect[] against unreasonable searches and seizures by . . . private individuals acting as instruments or agents of the Government." *United States v. Jarrett*, 338 F.3d 339, 344 (4th Cir. 2003). "The defendant shoulders the burden of establishing the existence of an agency relationship—a fact-intensive inquiry that is guided by common law agency principles." *United States v. Richardson*, 607 F.3d 357 (4th Cir. 2010) (internal quotations omitted). The question "necessarily turns on the degree of the Government's participation in the private party's activities." *Id.* (quoting *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989)). The Government's "passive acceptance" is not enough for a search to be unconstitutional; a defendant must show "Government participation" or "affirmative encouragement." *Id.* (quoting *Jarrett*, 338 F.3d at 344). The "key factors" are: "(1) whether the Government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation." *Id.* at 364 (quoting *Jarrett*, 338 F.3d at 344).

The Fourth Circuit has already considered and rejected the claim that, by monitoring and reporting user misconduct to NCMEC, an ESP is transformed into a government agent. *Id.* at 366. In *Richardson*, the defendant "believe[d] that AOL, functioning as a government agent, conducted a constitutionally impermissible search when it scanned his email communications for illicit images of child pornography without a search warrant." *Id.* at 363. The Court observed that "law enforcement agents did not actually participate in the search," did not "specifically

ask[] AOL to search," and did not "request that AOL aid in the investigation" part from compulsory legal process. *Id.* at 364-65. Nothing suggested that law enforcement was involved at all "until after AOL reported its discoveries to NCMEC." *Id.* at 365. Nothing "demonstrate[d] the existence of a *de facto* agency relationship between AOL and the Government." *Id.* at 365.

The Court also dismissed the idea that an ESP's mandatory compliance with the reporting scheme in 42 U.S.C. § 13032 transforms it into a government agent. *Id.* at 365-66 (rejecting the defendant's analogy to *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989)). The reporting requirement "neither directed AOL to actively seek evidence of child pornography in certain circumstances nor prescribed the procedures for doing so." *Id.* at 366. Quite the opposite: "Congress made abundantly clear that § 13032(b)(1) was not to be interpreted as requiring an ISP to monitor a subscriber's internet activity." *Id.* at 366-67; 42 U.S.C. § 13032 ("Nothing in this section may be construed to require a provider of electronic communication services or remote computing services to engage in the monitoring of any user, subscriber, or customer of that provider, or the content of any communication of any such person."). Consistent with regulations, AOL could even enter into subscriber agreements that "preclude monitoring." *Richardson*, 607 F.3d at 367. For those reasons, the mandatory reporting scheme "did not effectively convert AOL into an agent of the Government for Fourth Amendment purposes." *Id.*

The Fourth Circuit is in good company. Every court to consider the issue of whether a private electronic service provider acts as a government agent by

monitoring activity on its servers and reporting to NCMEC has soundly rejected the notion. *See United States v. Reddick*, 900 F.3d 636, 639 (5th Cir. 2018) (characterizing a PhotoDNA search for child pornography as a "private search"); *United States v. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013) ("AOL's decision on its own initiative to ferret out child pornography does not convert the company into an agent or instrument of the government for Fourth Amendment purposes. . . AOL's voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent."); *United States v. Cameron*, 699 F.3d 621, 637-38 (1st Cir. 2012) ("[I]f Yahoo! chose to implement a policy of searching for child pornography, it presumably did so for its own interests."); *United States v. Rosenschein*, 2020 WL 6680657, at *11 (D.N.M. November 12, 2020) (concluding that "neither Microsoft nor Chatstep was a government agent"); *United States v. Coyne,* 387 F. Supp. 3d 387, 396 (D. Vt. 2018) ("It is also clear that the three ESPs involved in these cases—Microsoft, Oath [Yahoo], and Chatstep—are not themselves agents of law enforcement."); *United States v. Rosenow*, 2018 WL 6064949, at *7-10 (S.D. Cal. Nov. 20, 2018) (holding that Yahoo "acted in a private capacity not subject to Fourth Amendment constraints"); *United States v. Stratton*, 229 F. Supp. 3d 1230, 1238 (D. Kansas 2017) (holding that Sony was not a government agent when it searched images stored on the defendant's PlayStation 3); *United States v. Miller*, 2017 WL 2705963, at *3-4 (E.D. Ky. June 23, 2017) (holding that Google is not a government entity); *United States v. DiTomasso*, 81 F. Supp. 3d

304, 309-311 (S.D.N.Y. 2015) (concluding that chat service provider Omegle had conducted a purely private search and was not acting as a government agent).

The defendant cannot carry his burden in this case. No evidence supports the theory that Microsoft acted as a government agent in reviewing and reporting the defendant's uploads. Regarding the first prong, as with *Richardson*, "no law enforcement agency specifically asked [Microsoft] to search" the uploads "or provided information about [the defendant] to cause" Microsoft to do so. 607 F.3d at 364. Likewise, nothing suggests "law enforcement agents were involved in the search or investigation of [the defendant's activity on BingImage] until after [Microsoft] reported its discoveries to NCMEC." *Id.* at 365. As for the second prong, "Microsoft has a long-standing commitment and legitimate business interest in child online protection." Ex. 3 ¶ 2. This includes avoiding "direct and indirect costs," decreasing the volume of consumer complaints, protecting its "image and reputation," and providing its customers with "safer and more secure online experiences." *Id.*; *see also Cameron*, 699 F.3d at 638 (stating that although combatting child pornography is a government interest, that does not also mean that an ESP "cannot voluntarily choose to have the same interest"). Consistent with the Fourth Circuit's holding in *Richardson*—and as district courts specifically concluded in *Coyne* and *Rosenschein*—Microsoft is not a government agent when it scans its servers and reports illegal files to NCMEC. As a private actor, NCMEC lawfully found and reported the child sexual abuse material that the defendant uploaded.

III. Even if it is a government agent, NCMEC did not expand the scope of Microsoft's search

The defendant next contends that even if Microsoft conducted a lawful private search, NCMEC should be treated as a government entity or agent and may have expanded Microsoft's search. Mot. 11-12.

Assuming for a moment that NCMEC should be treated as a government actor, it did not expand Microsoft's search in this case. Where a private search is followed by a search by a government actor, the question becomes to what degree the government search expanded the private search. *See Jacobsen*, 466 U.S. at 115; *United States v. Miller*, 152 F.3d 813, 815 (8th Cir. 1998) (concluding that a police search of defendant's apartment was lawful because it went no further than private search by a treatment facility). If a government actor substantially expands a private search, the second search may run afoul of the Fourth Amendment. *See United States v. Ackerman*, 831 F.3d 1292, 1306-07 (10th Cir. 2016) (finding a violation where NCMEC opened an email and viewed three attachments in addition to the one the ESP had reviewed).

Here, NCMEC's search did not exceed the scope of Microsoft's private search. Microsoft, a private actor, conducted the initial searches and submitted the two CyberTipline Reports, each addressing a single file of "apparent child pornography," Ex. 1, at 1, 6; Ex. 2, at 1, 6. Both Reports clearly state that the ESP conducted a full review: "Did Reporting ESP view entire contents of uploaded file? Yes." Ex. 1, at 4; Ex. 2, at 4; *see also* Ex. 3 ¶ 10. These two already-viewed files were all that Microsoft attached to the CyberTipline Reports, Ex. 4, 5 ¶ 13, and became the basis

of the search warrant, Ex. 6, at 6-7. Because the reports included no further content, no additional search by a government entity or agent—law enforcement or NCMEC—could have surpassed the scope of Microsoft's initial private search. *See United States v. Kendall*, 2019 WL 5782010, at *3 (E.D. Ky. Nov. 6, 2019) (finding no violation where "NCMEC did not exceed the scope of the search by Chatstep, a private actor"); *United States v. Stratton*, 229 F. Supp. 3d at 1238-40 (finding no evidence that NCMEC exceeded, rather than repeated, Sony's private search and concluding therefore that the Fourth Amendment did not apply to NCMEC's subsequent search). Government actor or not, NCMEC could not have conducted an unlawful search—the proverbial cat was out of the bag.

This Court, therefore, need not decide whether NCMEC is a government entity or agent. Still, it's worth noting that *Ackerman* is not precedential here, as the Fourth Circuit has not yet considered the issue. *See United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016) (concluding that NCMEC is a government entity or agent). The CyberTipline Reports expressly state that NCMEC is a "private, non-profit 501(c)(3) organization." Ex. 1, 3, at 1. It performs "its programs of work pursuant to its own private mission and independent business operations" and "does not act in the capacity of or under the direction or control of the government or law enforcement agencies." *Id.*

IV. Regardless, the good faith exception would apply.

Even if the Court were to reach the novel conclusion that Microsoft was a government agent such that law enforcement's later review of the same images

violated the Fourth Amendment, the evidence obtained by the search warrant would still be admissible under the good faith exception to the exclusionary rule.

The Supreme Court has repeatedly reaffirmed that exclusion should be a court's "last resort," not its "first impulse." *Herring v. United States*, 555 U.S. 135, 140 (2009). The "sole purpose" of the exclusionary rule "is to deter future Fourth Amendment violations." *United States v. Davis*, 564 U.S. 229, 236 (2011). And "the deterrence benefits of exclusion 'vary with the culpability of the law enforcement conduct' at issue." *Id.* at 238 (quoting *Herring*, 555 U.S. at 143). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring*, 555 U.S. at 147 (emphases added).

In cases involving warrantless searches, the Supreme Court has held that "an otherwise unconstitutional search undertaken in good faith as a result of uncertainty or a reasonable, if mistaken, belief about the law gives rise to a good faith exception to the exclusionary rule." *United States v. Coyne*, 387 F. Supp. 3d at 402 (citing *Heien v. North Carolina*, 574 U.S. 54 (2014)). Because "[t]o be reasonable is not to be perfect," "the Fourth Amendment allows for some mistakes on the part of government officials, giving them fair leeway for enforcing the law in the community's protection." *Heien*, 574 U.S. at 60-61 (internal citations and quotation marks omitted). This is particularly true when law enforcement actions are consistent with circuit precedent. "[S]earches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule." *Davis*, 564

U.S. at 239-41. "An officer who conducts a search in reliance on binding appellate precedent does no more than act as a reasonable officer would and should act under the circumstances." *Id.* at 241 ("The deterrent effect of exclusion in such case can only be to discourage the officer from doing his duty.").

Any error that may have occurred here does not meet the high bar for exclusion and should not result in suppression. TFO Morse acted in good faith reliance on well-settled law—both in the Fourth Circuit and elsewhere—that ESPs do not act as government agents by choosing to monitor their networks, even when they must report known violations to NCMEC. *See Richardson*, 607 F.3d at 365-67. Even if this Court were to conclude that intervening law undermined *Richardson*'s holding, suppression would remain inappropriate based on the good faith exception. *See United States v. Chavez*, 894 F.3d 593, 608 (4th Cir. 2018) (applying the good faith exception to cell phone records accessed before the Supreme Court held such seizures required a warrant); *United States v. Stephens*, 764 F.3d 327, 336-37 (4th Cir. 2014) (same, for the warrantless installation of a GPS device that was permissible at the time but later ruled unconstitutional).

[Remainder of page intentionally left blank]

CONCLUSION

WHEREFORE, for all the reasons set forth above, the United States requests the Court to deny the defendant's Motion to Suppress. In the absence of factual claims that could carry the defendant's burden of establishing an agency relationship between the government and Microsoft, the United States does not believe that a hearing is necessary.

Respectfully submitted, this the 10th day of December, 2021.

MICHAEL F. EASLEY, JR.
United States Attorney

By: /s/ Jake D. Pugh
JAKE D. PUGH
Assistant U.S. Attorney
Criminal Division
150 Fayetteville St., Suite 2100
Raleigh, NC 27601
Phone: (919) 856-4530
Email: jacob.pugh@usdoj.gov
S.C. Bar No. 100859

CERTIFICATE OF SERVICE

I hereby certify that I have this date served a copy of this document upon the defendant in this action either electronically or by placing a copy in the United States mail, postage prepaid, and addressed to counsel for defendant as follows:

J. Brad Polk
Attorney for the Defendant

This, the 10th day of December, 2021.

By: /s/ Jake D. Pugh
JAKE D. PUGH
Assistant U.S. Attorney
Criminal Division
150 Fayetteville St., Suite 2100
Raleigh, NC 27601
Phone: (919) 856-4530
Email: jacob.pugh@usdoj.gov
S.C. Bar No. 100859